AFRL-IF-RS-TR-2006-229
In-House Final Technical Report
July 2006

JOINT BATTLESPACE INFOSPHERE (JBI) DEMONSTRATION/VALIDATION EXERCISE

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. N683

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2006-229 has been reviewed and is approved for publication.

APPROVED: /s/

CHESTER J. MACIAG
Chief, Cyber Ops Branch
Information Grid Division

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, Jr.,Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JULY 2006	Final	Mar 03 – Mar 05

4. TITLE AND SUBTITLE
JOINT BATTLESPACE INFOSPHERE (JBI) DEMONSTRATION/ VALIDATION EXERCISE

5a. CONTRACT NUMBER
In-House

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
63760E

6. AUTHOR(S)
Chester J. Maciag

5d. PROJECT NUMBER
JBIH

5e. TASK NUMBER
00

5f. WORK UNIT NUMBER
15

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFGB
525 Brooks Rd
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington Virginia 22203-1714

AFRL/IFGB
525 Brooks Road
Rome New York 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2006-229

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA#06-482

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report describes in-house work performed by Air Force Research Laboratory (AFRL) in support of the Defense Advanced Research Projects Agency (DARPA) Organically Assured Survivable Information Systems Demonstration and Validation (OASIS Dem/Val) Program. The OASIS Dem/Val assessed how well the OASIS program technologies could perform in a real-world warfighter environment, by improving the security and availability of these systems to meet time-critical mission needs. The AFRL in-house effort supported the Dem/Val in the following ways: Development of an Air Operations Center (AOC) mission scenario; integration of existing "systems of record" and new Joint Battlespace Infosphere (JBI) technologies; code development of JBI 'concept applications' to demonstrate information feeds that were not practically reproducible in a lab environment; development of a realistic network architecture for the AOC systems and subsequent configuration management; development of scoring criteria for the two assessment exercises; hosting of the two exercises, and active participation in the White Team, which performed the scoring of the two assessment exercises and provided feedback on the Dem/Val's success to the DARPA Program Manager.

15. SUBJECT TERMS
Joint Battlespace Infosphere (JBI), Organically Assured Survivable Information System (OASIS), Air Operations Center (AOC), Dem/Val, DARPA, In-House, Survivable Exercise, Baseline Exercise.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chester J. Maciag
U	U	U	UL	10	19b. TELEPONE NUMBER (*Include area code*)

Table of Contents

1.0 Introduction

The Organically Assured Survivable Information Systems Demonstration and Validation (OASIS Dem/Val) Program developed a survivable implementation of the Air Force's Joint Battlespace Infosphere (JBI). During the design phase (Phase I), two teams (BBN Technologies and Boeing Phantom Works) competed to develop a better design to integrate many of the OASIS intrusion tolerance and survivability technologies in a secure system. The competitors also explored other research results, as well as commercially-available solutions, and new architectures to develop the first secure and survivable JBI. Each design was reviewed at the end of Phase I. At that time, a down-select occurred, with the superior design advancing to Phase II. BBN Technologies was selected to implement its Phase I design in Phase II. The goal of this second phase of the program was to develop a survivable JBI prototype that demonstrates the ability to operate through 12 hours of determined Red team attacks.

The participants for Phase II included:

- DARPA as the Program Manager
- BBN as the "developer/defender" Blue team and provider of the survivable JBI
- Cyber Defense Agency (CDA) as an "attacker" Red team, and
- The National Security Agency (NSA) and Sandia National Laboratory (SNL) collaborating as a second Red team
- Air Force Research Laboratory (AFRL) as the provider of the baseline JBI system and validation test bed facilities
- An Independent Evaluation Team (IET) of subject matter experts, and
- Federally Funded Research and Development Center (FFRDC), AFRL, and Naval Research Lab (NRL) representatives forming the "referee" White team.

The main components of the OASIS demonstration system are shown in Figure 1, which consisted of JBI core services and a collection of client applications. The JBI is a "publish, subscribe, and query" (PSQ) information distribution system for integrating client applications. JBI clients publish information objects (IO) to the JBI core. Clients that have matching IO subscription requests are then sent the IO in near real-time. Furthermore, previously published IOs that were archived are accessible to clients via queries to the JBI core. JBI clients communicate with the JBI core using a Common Application Programming Interface (CAPI) that provides the specifications for IOs and PSQ operations.

Figure 1 also depicts the exercise boundary, delineated by the red line, which designated the portions of the JBI that were within bounds for Red team attacks. In certain cases the user application was not fully integrated with the JBI client and required

operator intervention. These are depicted by the additional operator graphic (e.g., Theater Air Planner). Any applications or files that were outside of the red line were not part of the exercises.

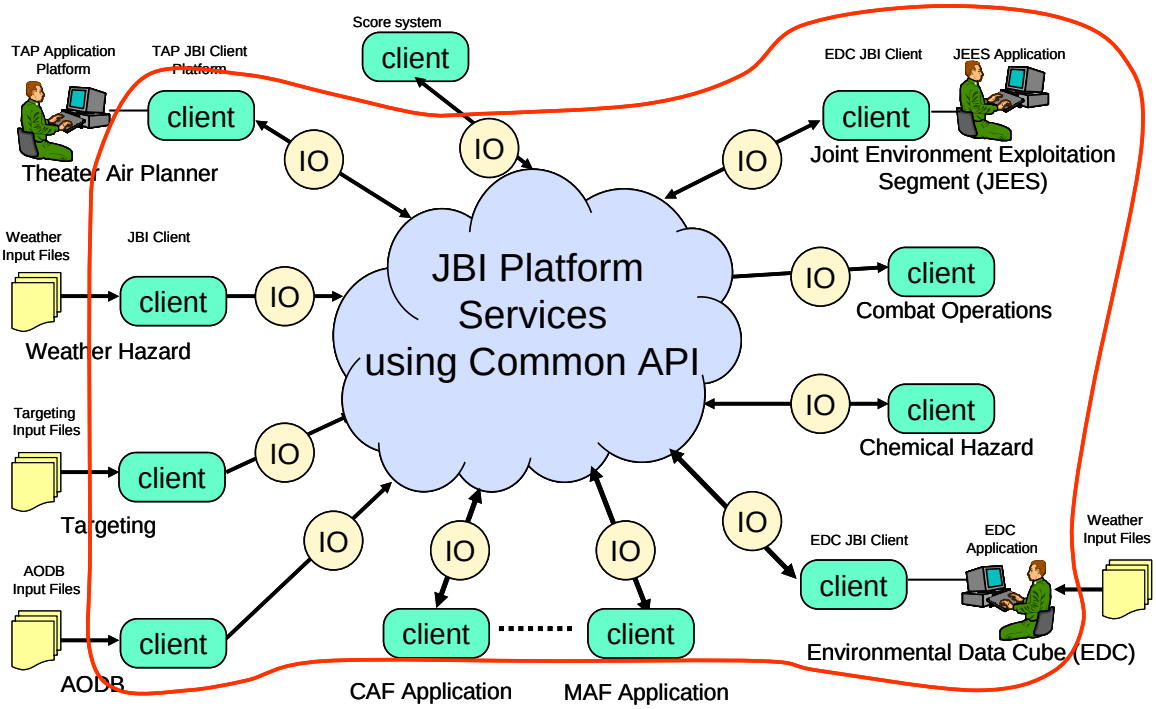


Figure 1 – OASIS Demonstration and Validation System

2.0 Summary of In-House Activities

2.1 Phase I

In this Phase, DARPA relied upon AFRL in-house engineers to develop a realistic Air Operations Center (AOC) scenario and supporting AOC applications that would serve as an 'exemplar' for BBN and Boeing development.

The scenario served as the baseline by which to determine exercise length, real-world data sources required, and necessary approximations. The real-world mission was modeled after US operations during the mid-90s Baltic conflict. The scenario was comprised of two 'threads'. Thread 1 was the theatre AOC generation of an Air Tasking Order (ATO) that relied upon weather, chemical, airspace, and targeting information. Thread 2 was a USTRANSCOM-initiated airlift mission that was scheduled to fly within the Baltic theatre and was required to be coordinated with the AOC planners. The 72-hour scenario and customary data exchanges and events were compressed into a 12-hour format. This was to permit the exercise to be conducted during duty hours, while still

providing the level of fidelity, data exchanges, and operator interactions necessary to make the experiment interesting.

AFRL/IF then sought to obtain the necessary AOC computer clients that would support the experiment. AFRL was able to obtain three systems-of-record for integration; the Joint Environmental Exploitation Segment (JEES), the Environment Data Cube (EDC); and Theater Battle Management Core Systems – Theater Air Planner (TBMCS-TAP). These systems were configuration-controlled, and minimal modification to them was made for the exercise. These were integrated with the JBI Core via an AFRL-developed API called the 'pub-sub graphical user interface' (pub-sub GUI). Other 'concept apps' were developed by the AFRL JBI team, to include:

- Combat Air Forces / Mobility Air Forces Mission Planning Clients
- Chemical Hazard Client
- Combat Operations Client
- Weather Hazard Client
- Air Operations Database (AODB) Client
- Modernized Integrated Database (MIDB) Client

For these AOC applications, the scenario was refined. The scenario now defined the sequence and timing of information objects (IOs) that would be passed between the applications, and when those IOs were expected to occur. This would be key to scoring in Phase II, as it would be critical to determine how long the Blue team could tolerate disruptions to the JBI before it would lead to mission failure.

The Dem/Val scenario and AOC applications were provided to the Phase I contractors in the Spring of 2004.

2.2 Phase II

After the Phase II down-select, DARPA made some modifications to the Dem/Val scoring methodology. Instead of allowing the possibility that the Red team might disrupt the AOC and cause early failure of the AOC mission threads, DARPA altered the scoring method to be more granular, and to increase the overall number of IOs exchanged in the scenario (to improve statistical relevance). To that end, AFRL:

- Identified the Information Objects that would be normally necessary to be passed between clients in order to complete the mission
- Developed the IO exchange sequence and timing windows
- Identified the 'critical' IOs that would irreparably 'break' a mission and cause failure
- Developed new scoring measurement methods, assuming the role of the AOC domain specialist. This was to help answer the question 'how do we quantify each IO exchange and score it, in order to measure percentage of

mission accomplished, and to determine if the DARPA Dem/Val goals have been met?'

- Identified and trained a cadre of warfighters to operate the AOC client applications in support of the mission threads of the scenario.
- Conducted the Baseline Exercise, to determine the degree of security and assurance offered by a relatively unsecured JBI exemplar, prior to subsequent testing of the survivable exemplar. The Baseline Exercise also served as a 'walk through' of the rigorous scoring challenges and procedures required for the Survivable Exercise

For the follow-on Survivable Exercise, AFRL:

- Addressed all logistical concerns for this on-site exercise, to include setup of Red and Blue team rooms, equipment configuration, and network connectivity.
- Developed the Dem/Val 'War Room'. This was a remote monitoring area where up to 20 observers and the White Team could monitor the Red and Blue team's actions and progress in real-time. All exercise computer screens could be viewed "on demand" to verify Blue Team defenses or Red Team attacks. Video cameras and audio feeds permitted live observation of team stress levels and AOC Operator reaction to Red Team attacks on AOC systems.
- Developed a graphical monitoring tool that would depict AOC progress in exchanging data products (IOs) in support of the mission threads. Would also indicate missed and delayed IOs. Proved to be one of the single-most useful progress indicators for the survivable experiment.

3.0 Lessons-Learned and Conclusions

As a result of the OASIS Dem-Val Exercises and In-House effort, the following lessons were learned:

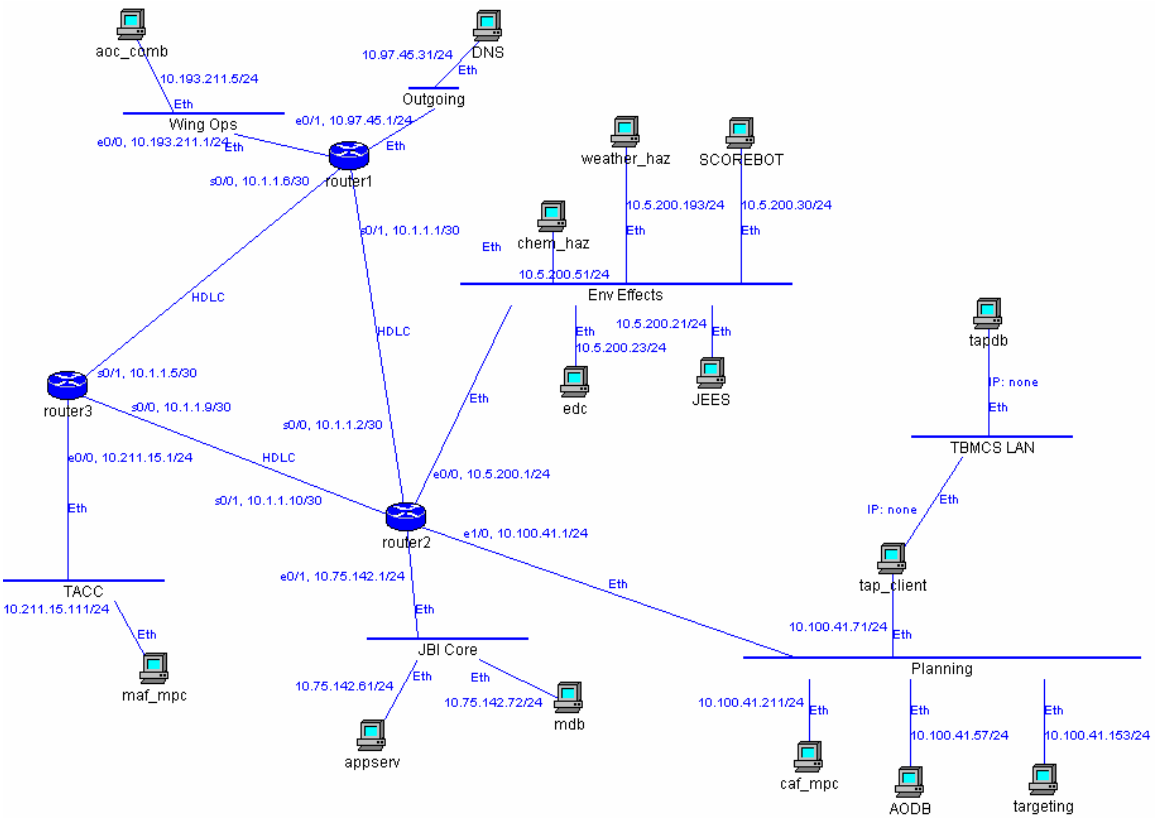
- Complex, monolithic applications can be broken up into smaller, more manageable pieces using the JBI. For example, the in-house effort demonstrated that it was possible to update TBMCS's legacy AODB and MIDB databases via a very simple JBI application-programming interface (API). This interface, known as the pub-sub GUI, allowed easy publishing of TBMCS data into the JBI, as well as easy subscription of JBI updates back into TBMCS. Similarly, the JEES/EDC legacy applications were integrated with TBMCS through the JBI core and the pub-sub GUI API. AFRL was able to demonstrate the rapid integration of these legacy applications for a mere fraction of the cost (about $100K) of what it would take to perform a new code development and update the configuration baselines.
- Legacy application re-architecting and integration costs could be dramatically reduced with the use of a JBI. Portions of TBMCS and EDC/JEES were easily added to the information space via information objects. Again, if you don't have

to change the configuration baseline of the application itself, you can save a lot of software regression testing and costs associated with updating baseline documentation.

- Constituent parts of a legacy information system need not care if they are platform-local or distributed. Again, the TBMCS example is cited, in which AFRL was able to break apart the functionality of MIDB and AODB, and hypothetically site these databases practically anywhere on the AF enterprise. This could afford the AF the ability to create fault-tolerance through replication of databases, as well as enhanced physical survivability of these databases by not requiring them to exist in the theatre of battle itself.

.

APPENDIX A -
OASIS Dem/Val Baseline Exercise Network Diagram



Notes:

- This diagram only captures the production network. All production machines that contain a JBI client also have a connection to the out of bounds 'Scoring Network'.
- The TBMCS LAN was 'out of bounds' for Red Team attack, since we already have a wealth of information on TBMCS vulnerabilities.
- The Red team connected via an Ethernet connection on the Env Effects LAN, to simulate an insider threat and not waste time trying to defeat a firewall. This was to spend the most amount of time learning about the Baseline JBI's vulnerabilities.